## REMARKS

Claims 1-19, all the claims pending in the application, stand rejected. Applicants have amended each of claims 1-19 in order to state the invention in a manner that is more consistent with U.S. practice. In particular, claim 1 has been amended to focus on the standard access control system where there is no direct connection to the short range transmitter and the short range transmitter is an independent unit.

### *Claim Rejections - 35 U.S.C. § 101*

**Claims 18-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.** This rejection is traversed for at least the following reasons.

The Examiner provides an example of acceptable language under 35 U.S.C. 101 as being "a computer readable medium storing a computer program...". Applicants have adopted the Examiner's suggestion.

**Claims 9-15 and 17-18 are rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101.** This rejection is traversed for at least the following reasons.

Applicants have amended the claims in order to set forth steps in accordance with U.S. practice.

### *Claim Rejections - 35 USC § 112*

**Claims 9-15 and 17-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite**. This rejection is traversed for at least the following reasons.

The Examiner notes that claims 9-15 and 17-18 are directed to a method related to the use of an access control system, but asserts that the claims do not set forth any steps involved in the method/process.

Applicants have amended the claims to state the structures that define the environment of the invention and then define the steps involved in the method of using those structures. Applicants believe that the claims now are in proper form under U.S. practice.

The Examiner also notes that claim 17 recites the limitation "time recording system" in line 2, and asserts that there is insufficient antecedent basis for this limitation in the claim. The claim has been amended to remove this basis for rejection.

***Claim Rejections - 35 USC § 103***

**Claims 1-7 and 9-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Straumann et al. (7,196,610) in view of Kniffin et al. (6,072,402).** This rejection is traversed for at least the following reasons.

**Claim 1**

Regarding independent claim 1, the Examiner asserts that Straumann et al. disclose an access control system having a standard access control system (Fig. 1) through which plural access points can each be controlled via individual physical locking mechanisms (device 1, 1') each connected to an electromechanical lock 15, which control access doors 3, 3,' and has at least one reader and controllers. The Examiner asserts that the access control device 1 further comprises a communication module 11 (col. 5, line 64-col. 6, line 5), an access control module 13 (col. 6 lines 25-47) and an ID module 12. With reference to col. 5 line 67-col. 6 line 18, the system is alleged to have a short-range transmitter provided at one specified location for transmitting access-point-specific identification information to a mobile telephone 2, which the Examiner asserts is located in the reception area of the transmitter, and is used at least indirectly to control the access control at a specific associated access points.

However, the disclosure of Straumann et al does not teach the claimed absence of a direct connection between the mobile unit and the access control unit.

**Straumann et al**

Straumann's Operation Is Limited To Direct Communication Between Mobile and Control Device

Straumann et al describes a technology in which a mobile communication terminal (mobile phone) 2 is in communication with a local access control device 1 to operate lock 15. According to Straumann, the mobile communication terminal must handle and store an access code (see for example column 3, lines 19-26), and the communication for triggering of lock 15 only takes place between the mobile communication terminal 2 and the local access control device 1.

Straumann explicitly intends to avoid any further networking and interconnections between the devices. As explained at column 3, lines 47-51, authentication and identification communication takes place only between the local access control device 1 and the mobile communication terminal 2

Further, in Fig. 1 of Straumann the only connection to the access control unit 1 is via a radio link to the mobile communication terminal 2. There is no connection between the central control server 4 and the local access control unit 1.

With regard to the specific method of system operation taught by Straumann in the illustration of Fig. 2, as described at column 8, line 12 - column 9, line 30, authorization is established only by communication between the mobile communication terminal 2 and the local access control device 1. In order to be able to do so in a safe way, it is necessary that digital certificates are or stored, and can be verified, modified and handled on both devices, i.e. on the local access control device 1 and on the mobile communication terminal 2.

As compared to Applicants' invention, the structure and process in Straumann et al presents an undue burden.

Straumann's Central Control Has A Limited Function Relevant To Authorization

In Straumann, there is an access control central unit 4, but this unit only acts once, and at the beginning of the authorization process. Specifically, unit 4 only acts to authorize the mobile communication terminal once, by providing the access code; however, the actual process of authorization and triggering the unblocking of the local lock exclusively takes place by communication between the mobile communication terminal 2 and the local access control device 1.

Straumann's System Is Deficient

Because of the foregoing limitations on the roles of the access control device 1, the mobile communications terminal 2 and the access control central unit 4, access code data must be stored and handled on the mobile communication terminal. This necessitates complicated devices.

Also, the local transmitter 11 in Straumann must be connected with the local control. If this were not the case, it would not be possible to open the lock 15 using the mobile communication terminal.

Straumann's System is Different

In view of the above the subject matter of claim 1 is clearly distinguished from Straumann in at least the following features:

• the access control server of the present invention is in direct contact with the local controllers; and

• a short range transmitter, in the form of an independent unit with no direct connection to the standard access control system, is provided at one specified location. The transmitter transmits access point specific identification information in such a manner that this is received by a mobile telephone which is located in the reception area of the transmitter and is used at least indirectly by this to control the access control at a specific associated access point.

**Claim 9**

The foregoing differences are embodied in independent method claim 9, as amended. First, the claim sets forth the environment of the recited method, which includes the structure of amended claim 1. Second, as to the method steps, the claim expressly requires that, due to the independence of the transmitter, and due to the lack of a direct connection to the standard access control system, transmission occurs only of access point specific identification information for receipt by the mobile phone, but there is no participation in the authentication and the unlocking process.

The mobile phone after receipt of the corresponding signal subsequently must use the mobile phone network, the corresponding mobile phone server, and an access control server. This, in turn by means of connection to the local controller, opens the lock.

As a result the processes which have to be carried out on the mobile phone are much simpler and, in particular, do not involve the calculation or the storage of an access code or certificate, as in Straumann et al.

Further, due to the complete control by the claimed access control server over the access process, an increased security is achieved.

Finally, since the access control system and, therefore the local controller, are not connected to the local short range transmitter, the transmitter can be located at a specific point not necessarily in close vicinity of the local control device. As a result, the authorization can occur well ahead of the control device for access points using vehicles or the like.

**Kniffin et al**

The Examiner admits that Straumann et al. fails to disclose several claim limitations, including (1) at least one access control server, which carries out central management of the access data and is connected to the respective controllers and (2) at least one mobile telephony server connected to the access control server, which is at least indirectly able to send data via a mobile telephone network to mobile telephone subscribers, and to receive data from mobile telephone subscribers.

The Examiner looks to Kniffin et al. for a disclosure of at least one access control server, which carries out central management of the access data and is connected to respective controllers (clearinghouse 54 transmits an RF signal to the identified lock and causes it to briefly make itself susceptible to being unlocked, as disclosed in fig. 3 and further disclosed in col. 7 lines 20-30). The Examiner also looks to Kniffin for at least one mobile telephony server connected to the access control server, which is at least indirectly able to send data via a mobile telephone network to mobile telephone subscribers, and to receive data from mobile telephone subscribers. The Examiner concludes that it would have been obvious to one of ordinary skill in the art at the time of invention to modify the access control device as disclosed by Straumann et al. to connect to an access control server (clearinghouse) as disclosed by Kniffin et al.

Two Separate Modes of Operation

Kniffin et al teaches two separate and not interrelated processes. In a first process, as illustrated in Figure 3 and described at column 7, lines 20-29, the mobile phone 52 connects to a central access control server, which subsequently, after verification, triggers the local controller via a wireless connection. Correspondingly in this first mode of operation there is no direct connection established between, the transmitter of the local controller and the mobile phone.

In a second process, as illustrated in Figure 3 and described at column 7, lines 36-41, the mobile phone (52) does not contact the access control server, but directly contact the local access control device. Subsequently, as outlined in lines 42-49, the local controller receives authorization from the access control server.

Clearly, in the absence of any direct connection between the With a specific process as defined in claim 1 and 9 is therefore not disclosed in Kniffin nor is it suggested by Kniffin.

Correspondingly therefore there is no suggestion in either Straumann or in Kniffin (1) to have a local short range transmitter providing only localization information to the mobile phone and (2) to then have the mobile phone initiate the unblocking process by means of the mobile network, the central access control server, and the access control server subsequently authorizing to unlock the local controller.

To omit an independent local short range transmitter in each of the two disclosures would indeed make sense. On the other hand, Applicants submit that the processes and methods as disclosed in Straumann or Kniffin would not even work at all if the local short range transmitter would be independent from the access control system and thus of the local controller.

**Claims 2-7 and 10-15**

The foregoing claims have been amended in order to provide consistency with parent independent claims 1 and 9. Thus, these claims also should be patentable.

**Claims 16**

Claim 16 is an independent apparatus claim directed to a time recording system. Claim 16 has the limitation that "a short-range transmitter provided for at least one authorized area, which transmitter is in the form of an independent unit, with no direct connection to the standard time recording system, and is operative to transmit area-specific identification information in such a way that the information is received only by a mobile telephone which is located in the immediate vicinity of the authorized area, and is used by said mobile telephone at least indirectly for the manipulation of the time data." This limitation is not found in the prior art, as asserted previously with regard to claims 1 and 9.

**Claim 17**

Claim 17 is an independent method claim that contains substantially all of the limitations of claim 16 as the environment for a method for time recording, including the transmitter is in the form of an independent unit, with no direct connection to the standard time recording system. The claim would be patentable for the reasons given for claim 16.

**Claims 18 and 19**

These two claims depend from claim 9 and would be patentable for the reasons given for claim 9.

**Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Straumann et al. (7,196,610) in view of Kniffin et al. (6,072,402) and further in view of Want et al. (2003/0114104).** This rejection is traversed for at least the following reasons.

The Examiner repeats the assertion that the combination of Straumann et al. and Kniffin et al. teaches all the limitations as claimed in parent claim 1, but admits that the combination fails to disclose that the standard access control system also allows access control using means without mobile telephony, in particular based on RFID technology.

The Examiner looks to Want et al. for a disclosure that each portable electronic device 14, 16, 18 includes a radio frequency identification (RFID) tag 24 and, accordingly, the computer access device 12 includes a complimentary REID reader 26 as disclosed in fig. 1 and paragraph 11.

Want et al, however, does not remedy the deficiencies of Straumann et al and Kniffin et al, as already described. Thus, this claim would be patentable for the reasons given for parent claim 1.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

*/Alan J. Kasper/*

Alan J. Kasper
Registration No. 25,426

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860
WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: March 20, 2008